Cassandra Crossing/ Tor c'è

(26)— Addio filtri sugli IP, addio controlli sul Web.. c'è TOR. Installarlo è questione di un attimo. Se poi si dispone di una flat ADSL in…

Cassandra Crossing/ Tor c'è

(26)— Addio filtri sugli IP, addio controlli sul Web.. c'è TOR. Installarlo è questione di un attimo. Se poi si dispone di una flat ADSL in poche mosse si può moltiplicare l'efficienza della rete.

10 marzo 2006— La vicenda della censura dei siti per il gioco d'azzardo da parte dei Monopoli di Stato ha prodotto molti effetti; l'ultimo è l'aver determinato la scelta della "monografia" di oggi, dedicata a TOR (The Onion Router), la più recente novità tra le risorse per la privacy in rete.

TOR è un sistema per utilizzare applicazioni internet, ed in particolare browser web, mantenendo un alto grado di privacy. Usando TOR è possibile navigare in forma praticamente anonima, e contemporaneamente azzerare le possibilità che i dati di navigazione possano essere memorizzati nell'ambito di attività di Data Retention svolte da ISP ed altri enti.

Tecnicamente è una rete di proxy anonimizzanti (onion router o router TOR) che aprono connessioni TCP su richiesta di un client TOR, che a sua volta riceve la richiesta da una normale applicazione come un browser web. Client TOR ed applicazione risiedono sul pc.

TOR ha una architettura SOCKS, e puo' collegarsi in cascata con altri programmi per la privacy; una scelta molto utile e popolare è quella di abbinarlo a

Privoxy, un proxy filtrante che permette di controllare le informazioni in uscita ed in ingresso dal pc, ad esempio togliendo il numero della carta di credito o bloccando gif animati e pop-up. I due programmi lavorano insieme senza quasi nessuna configurazione.

TOR è disponibile su tutte le piattaforme più diffuse, Windows, Linux, Mac e vari dialetti Unix. E' particolarmente facile da installare ed è promosso anche da EFF (Electronic Frontier Foundation)

La sua documentazione è molto completa e le parti principali sono disponibili in italiano.

Esistono anche distribuzioni già pronte standalone, come TORPark o TORCP.

TORPark, già oggetto di un precedente articolo di PI consta di un unico file zip per ambiente Windows. Comprende al suo interno, in un unica directory, sia TOR che una versione completa del browser Mozilla Firefox.

Per usarlo bisogna scompattarlo su una chiave USB (ma funziona anche da disco) e lanciare l'eseguibile torpark.exe. Si apre Firefox ed è possibile navigare in anonimato e scaricare file e bookmark sulla chiavetta, senza lasciare dati o file temporanei a giro. Alla fine basta lanciare torkill.exe, sfilare la chiavetta e rimettersela in tasca, con buona pace di chi vuole violare la privacy altrui.

Una nota a margine richiamando un fatto recente: nessuna della azioni censorie che agiscano sul DNS o IP di siti da censurare ha alcun effetto sulla navigazione effettuata tramite TOR.

Per finire alcune note a margine.

TOR è un progetto di software libero che, benché sia stato anche finanziato da EFF nel 2005, è ora di nuovo sostenuto solo dai suoi sviluppatori. Aiutare questi progetti è interesse di ciascuno, perché non esistono cose come pasti gratis; contribuire tramite una visita a questa pagina è quindi consigliato.

I router TOR usano parecchie risorse di banda; aprire una connessione di 10 kByte/sec ne costa da 30 a 40. A parità di router (server) esistenti, e quindi di banda disponibile, al crescere egli utenti la banda per ciascuno tende rapidamente a zero. L'unica soluzione è quella di creare nuovi server, cosa alla portata di chiunque abbia un'ADSL flat e voglia donare una frazione della propria banda. Trovate le istruzioni qui.

Se poi tutto quello che avete disponibile è un po' di tempo, qui trovate indicazioni su come spenderlo utilmente per contribuire al progetto TOR.

Chi stesse scegliendo un lavoro di tesi di laurea di argomento informatico potrebbe valutare alcuni degli sviluppi in corso come argomento. Scrivete a Roger Dingledine o a me se siete interessati.

Originally published at punto-informatico.it.